Analisis Penerapan Firewall Nftables Sebagai Sistem Keamanan Server Pada Mesin Virtualisasi

Malik Purwoko[1], Hamzah Hilal[2]

[1]*Badan Kajian Teknologi Polimer, BPPT, Jakarta*
[2]*Badan Pengkajian dan Penerapan Teknologi Republik Indonesia, Jakarta*
malik.purwoko@sentrapolimer.id[1], hamzah.hilal@bppt.go.id[2]

Abstrak

Teknologi virtualisasi telah mengubah arah revolusi industri komputer dengan cara penurunan biaya-biaya modal, biaya operasional, ketersediaan layanan yang lebih tinggi dan mekanisme perlindungan data. Balai Teknologi Polimer telah menerapkan server-servernya di dalam mesin virtualisasi., pada penelitian ini dilakukan analisa dan penerapan firewall dengan menggunakan nftables pada mesin virtualisasi. Nftables adalah firewall generasi baru di sistem operasi linux yang siap menggantikan iptables sebagai firewall. Penelitian ini menguji kinerja firewall nftables terhadap serangan DDoS (Distribution Denial of Service). Pengambilan data pengujian DDoS dilakukan sebanyak 30 kali dengan tools yang ada di linux, yaitu htping3 dan wireshark. Skenario 1 tanpa gangguan DDoS diambil data sebanyak 10 kali, skenario 2 dengan DDoS gangguan ke server sebanyak 32000 byte dengan 3 komputer sebanyak 10 kali. Dan terakhir skenario 3 dengan gangguan DDoS sebanyak 65000 byte dengan 6 komputer sebanyak 10 kali juga. Hasil penelitian menunjukan saat tidak ada serangan DDoS server berjalan baik dengan troughput yang besar dan pemakaian sumber daya CPU (%) yang kecil. Namun setelah dilakukan serangan DDoS terjadi penurunan nilai troughput dan pemakaian CPU yang besar. Semakin besar jumlah serangan maka semakin menurunkan nilai troughput dan makin membesarnya pemakaian sumber daya CPU dari server firewall.

Keywords: Frewall; Virtual mesin; DDoS; Linux; nftables; Troughput; CPU Usage

DOI: 10.22441/incomtech.v9i1.5676

1. PENDAHULUAN

Dalam perkembangan teknologi sekarang ini banyak perusahaan yang sudah menggunakan server dengan teknologi virtualisasi. Beberapa kemungkinan yang sebelumnya diadaptasi dari pendekatan infrastruktur fisik seperti satu *hardware* (*processor*, *memory*, *network*, *storage*), satu *operating system* dan satu aplikasi, saat ini telah berubah menggunakan pendekatan infrastruktur virtual, seperti satu

hardware, *multi operating system* dan multi aplikasi [1]. Begitupun di Balai Teknologi Polimer yang menerapkan server-servernya di dalam server mesin virtualisasi, dimana server-server ini sebelumnya berada dalam satu jaringan lokal staff tanpa ada pengamanan di depan server tersebut. Pada penelitian ini dipilih jenis pengamanan server pada mesin virtualisasi dengan menggunakan linux server di dalam mesin virtualisasi tersebut untuk dijadikan firewall. Diantara banyak firewall di linux, *firewall* generasi baru dilingkungan sistem operasi linux yaitu nftables akan di implementasikan sebagai pengaman server di mesin virtuliasi Balai Teknologi Polimer. Penyebab utama dari masalah jaringan adalah tindak penyalahgunaan teknologi oleh orang-orang yang tidak bertanggung jawab dengan tujuan memanfaatkan fasilitas jaringan pihak lain untuk kepentingan pribadi maupun kelompok [2]. Pentingnya peranan firewall dalam mengamankan jaringan lokal terhadap kemungkinan serangan dari pihak-pihak yang tidak bertanggung jawab memberikan kontribusi penting dalam keamanan jaringan. Kinerja *firewall* secara umum bergantung pada manajemen aturannya, firewall bisa sangat bermanfaat jika digunakan sebagai *filter* menuju kesemua akses internet dari dan ke system yang melewatinya.

Diantara banyaknya serangan yang sering terjadi di internet adalah serangan DDoS (*Distribution Denial of Service*), merupakan jenis serangan jaringan komputer yang dapat mengakibatkan server tidak mampu melayani permintaan user, hingga menyebabkan jaringan komputer menjadi down. Serangan pada firewall juga biasanya dilakukan dalam bentuk penyusupan dengan menggunakan berbagai macam jenis serangan jaringan komputer melalui *tools* yang dibuat secara mandiri ataupun *tools* yang di dapat dari internet [3]. Pada penelitian sebelumnya terkait nftables adalah perbandingan performa latensi dan troughput dari iptables dengan nftables, dan dalam saran penelitian tersebut menyebutkan bahwa peluang penelitian kedepan untuk iptables dan nftables adalah membandingkannya dengan serangan DDoS [4]. Berdasarkan paparan hasil dari peneliti di atas dan atas kebutuhan akan implementasi firewall untuk mengamankan server di Balai Teknologi Polimer, untuk itulah disini penulis mencoba membuat penelitian dengan melakukan implementasi dan pengujian firewall nftables didalam lingkungan virtualiasi terhadap serangan DDoS (*Distribution Denial of Service*) yang menggunakan htping3 untuk serangannya dan *wireshark* sebagai analisanya.

2. KEAMANAN JARINGAN

Analisis adalah mengelompokkan, membuat suatu urutan, memanipulasi, serta menyingkatkan data sehingga mudah dibaca [5]. Jaringan komputer adalah hubungan dari sejumlah perangkat yang dapat saling berkomunikasi satu sama lain. Perangkat yang dimaksud pada definisi ini mencakup semua jenis perangkat komputer (*computer desktop*, komputer jinjing, *smartphone*, *tablet*) dan perangkat penghubung (*router*, *switch*, *modem* dan *hub*) [6].

Adanya keamanan jaringan maka para pengguna berharap bahwa pesan yang dikirim dapat sampai dengan baik ke tempat yang dituju tanpa mengalami adanya kecacatan yang diterima oleh si penerima, misalnya saja adanya perubahan pesan. Biasanya jaringan yang aksesnya semakin mudah, maka keamanan jaringannya semakin rawan, namun apabila keamanan jaringan semakin baik maka pengaksesan jaringan juga semakin tidak nyaman. Analisa kinerja pada jaringan komputer membicarakan sifat dasar dan karakteristik aliran data, yaitu efisiensi daya-kerja,

penundaan dan parameter lainnya yang diukur untuk dapat mengetahui bagaimana suatu pesan diproses di jaringan dan dikirim lengkap sesuai fungsinya, yaitu;

1. Dapat menyempurnakan level layanan pemeliharaan.
2. Dapat mengenali potensi kemacetan.
3. Dapat mendukung pengendalian operasional jaringan, admunistrasi dan merencanakan kapasitas.

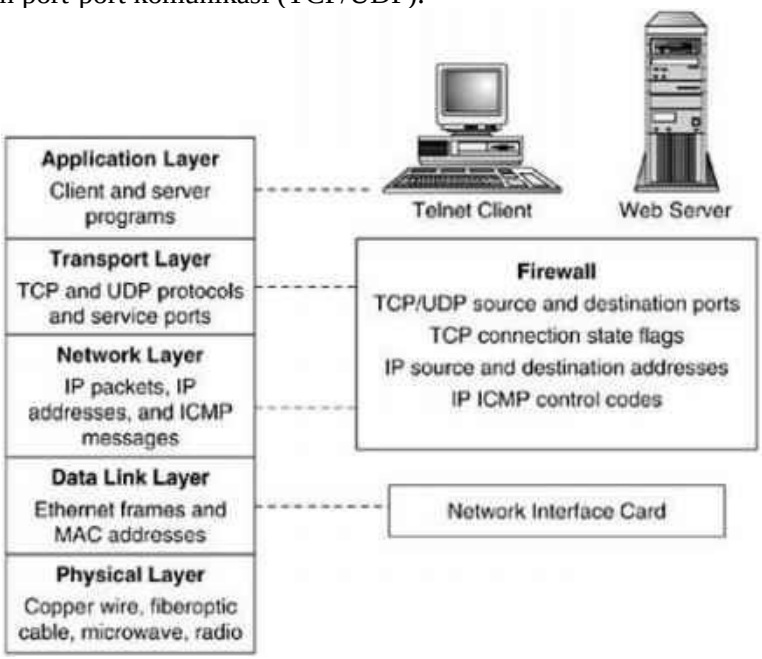
Aspek keamanan Informasi menurut William Stallings [7] :

a. *Privacy / Confidentiality*, yaitu menjaga informasi dari orang yang tidak berhak mengakses data.
b. *Integrity*, yakni informasi tidak boleh diubah tanpa seijin pemilik informasi.
c. *Authentication*, yaitu metoda untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah orang yang dimaksud.
d. *Access control*, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi

Selain hal di atas, masih ada dua aspek lain yang berkaitan dengan *electronic commerce*, yaitu *access control clan non-repudiation.*

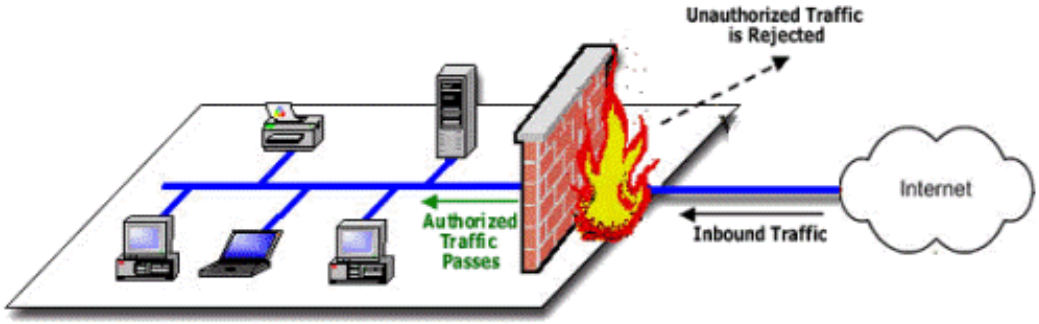
2.1. Firewall

Istilah *firewall* dalam kaitannya dengan Teknologi Informasi (TI) mungkin pertama kali digunakan pada tahun 1992 ketika Marcus J. Ranum menerbitkan sebuah makalah bernama "*A Network Firewall*"[8]. *Firewall* adalah sebuah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. Umumnya, sebuah firewall diimplementasikan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (*gateway*) antara jaringan lokal dan jaringan lainnya. Firewall di gunakan untuk membatasi koneksi dengan cara menolak atau mengijinkan koneksi tertentu. Sebagai contoh, koneksi dengan tujuan *webserver* dengan menggunakan port 80 ke dalam jaringan DMZ tentu saja di ijinkan karena server kita menyediakan layanan tersebut. Namun koneksi lain seperti *telnet*, ataupun layanan yg tidak di sediakan oleh server akan di tolak, hal ini tentu saja akan menambah keamanan system yg kita bangun. Bagian lapisan firewall dijelaskan seperti pada Gambar 1, layer 3 adalah layer yang mengurus masalah pengalamatan IP, dan layer 4 adalah menangani permasalahan port-port komunikasi (TCP/UDP).



Gambar 1. Penempatan firewall dalam model referensi TCP IP

Jika di ilustrasikan, firewall pada dasarnya bertindak seperti petugas imigrasi yang melakukan pengecekan terhadap lalu lintas orang dan barang ke suatu negara. Apabila orang atau barang tersebut membawa dokumen yang sah dan legal, akan di ijinkan untuk masuk, namun sebaliknya, bila tidak di lengkapi dengan dokumen yg sah dan legal maka di tolak masuk. Seperti pada Gambar 2, *Firewall* akan bertindak sebagai pertahanan pertama *host* terhadap serangan dari luar [9]. *Firewall* merupakan perangkat jaringan yang berada di dalam kategori perangkat Layer 3 (*Network layer*) dan *Layer 4* (*Transport layer*) dari protokol 7 OSI layer.



Gambar 2. Model Umum Firewall

Fungsi firewall, antara lain:

a. Mengontrol dan mengawasi paket data yang mengalir di jaringan.
   Firewall harus dapat mengatur, memfilter dan mengontrol lalu lintas data yang diizin untuk mengakses jaringan privat yang dilindungi firewall. Firewall harus dapat melakukan pemeriksaan terhadap paket data yang akan melawati jaringan privat.Beberapa kriteria yang dilakukan firewall apakah memperbolehkan paket data lewati atau tidak, antara lain :
   - Alamat IP dari komputer sumber
   - Port TCP/UDP sumber dari sumber
   - Alamat IP dari komputer tujuan
   - Port TCP/UDP tujuan data pada komputer tujuan
   - Informasi dari *header* yang disimpan dalam paket data
b. Melakukan autentifikasi terhadap akses.
c. Aplikasi proxy
   Firewall mampu memeriksa lebih dari sekedar *header* dari paket data, kemampuan ini menuntut firewall untuk mampu mendeteksi protokol aplikasi tertentu yang spesifik.
d. Mencatat semua kejadian di jaringan
   Mencatat setiap transaksi kejadian yang terjadi di firewall. Ini memungkinkan membantu sebagai pendeteksian dini akan kemungkinan penjebolan jaringan.

Firewall perangkat lunak dibagi menjadi empat kategori utama, seperti tercantum di bawah ini:

A. Paket Filtering Firewall

Firewall penyaringan paket menerapkan seperangkat aturan dan memeriksa setiap paket untuk menentukan apakah akan meneruskan paket atau jatuh ke tujuan

tertentu. Firewall biasanya dikonfigurasikan untuk memfilter paket yang menuju ke dua arah, masuk dan keluar. Filter paket mengizinkan atau menolak lalu lintas jaringan berdasarkan informasi berikut:

- Sumber alamat IP dan alamat IP tujuan.
- Protokol, seperti TCP, UDP.
- Port sumber dan port tujuan.
- Arahan (masuk atau keluar).
- Antarmuka fisik tempat paket dilalui.

B. Gateway Level Circuit gateway

Circuit level bekerja pada lapisan sesi model OSI, atau lapisan TCP dari model TCP / IP Firewall ini memonitor *handshake* TCP di antara paket untuk menentukan apakah sesi yang diminta diizinkan. Hal ini memberi keuntungan karena menyembunyikan informasi tentang jaringan pribadi yang dilindungi dan tidak memfilter paket individual.

C. Gateway Tingkat Aplikasi

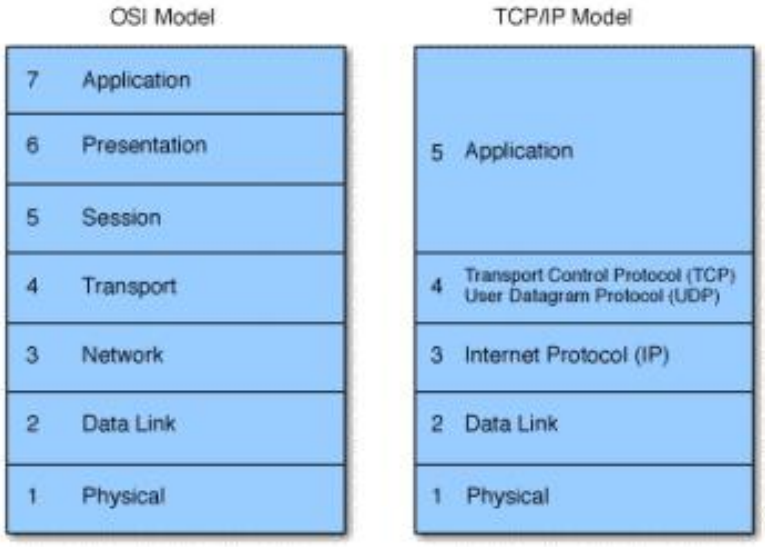
Gateway tingkat aplikasi, juga disebut proxy, mirip dengan gateway tingkat sirkuit kecuali bahwa mereka adalah aplikasi spesifik. Dengan kata lain, paket masuk atau keluar tidak dapat mengakses layanan yang tidak ada proxy. Misalnya, jika gateway aplikasi dikonfigurasi untuk menjadi proxy web, itu tidak akan memungkinkan untuk menggunakan FTP, Telnet atau lalu lintas lainnya. Firewall ini digunakan untuk mencatat aktivitas pengguna dan login. Ini menawarkan lebih banyak keamanan, tetapi memiliki dampak signifikan pada kinerja jaringan. Ini karena sakelar konteks, yang memperlambat akses jaringan secara dramatis.

D. Firewall Inspeksi Multilayer Stateful

Firewall inspeksi multilayer *stateful* menggabungkan aspek-aspek dari ketiga jenis firewall yang disebutkan di atas. Ini menyaring paket pada lapisan jaringan untuk menentukan apakah paket sesi diperbolehkan dan mengevaluasi isi paket pada lapisan aplikasi firewall multilayer *stateful* memungkinkan koneksi langsung antara klien dan host dan menawarkan lebih banyak keamanan, kinerja dan transparansi kepada pengguna akhir.

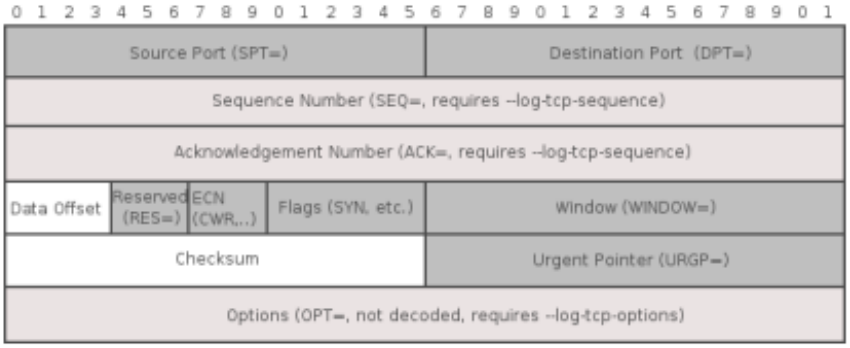
Untuk memahami cara kerja firewall, hal pertama adalah memiliki pengetahuan tentang bagaimana berbagai lapisan jaringan berinteraksi [10]. Arsitektur jaringan dirancang dengan model tujuh lapis. Setiap lapisan memiliki tanggung jawabnya sendiri dan menangani data dengan cara yang jelas. Gambar 3 menyajikan arsitektur lapisan jaringan.

Firewall beroperasi pada lapisan yang berbeda untuk menggunakan kriteria yang berbeda untuk membatasi lalu lintas. Dalam model OSI, ini adalah lapisan jaringan, dalam model TCP / IP itu adalah lapisan protokol Internet. Lapisan ini berkaitan dengan perutean paket ke tujuan mereka. Pada lapisan ini firewall menentukan apakah suatu paket berasal dari sumber yang tepercaya, tetapi tidak berkaitan dengan apa yang dikandungnya atau paket apa yang terkait dengannya. Beberapa firewall beroperasi pada layer transport dan tahu lebih banyak tentang suatu paket, yang kemudian menghasilkan akses hibah atau ditolak tergantung pada kriteria yang ditentukan.



Gambar 3. OSI dan model TCP / IP

Paket memiliki header IP yang diikuti oleh tajuk TCP, UDP atau ICMP, Header TCP dan UDP diikuti oleh pesan aplikasi. Pemeriksaan paket berfokus pada isi tajuk IP, TCP, dan UDP. Header IPv4 TCP dan UDP seperti ditunjukkan pada Gambar 4 dan 5.



Gambar 4. Header IPv4 TCP

Gambar 5. Header IPv4 UDP

Ketika sebuah paket memasuki firewall, ia mulai mencocokkan informasi paket dengan aturannya. Aturan penyaringan paket didasarkan pada:

- NIC spesifik
- Alamat IP host
- Alamat IP sumber dan tujuan lapisan jaringan
- Transport port-port layanan TCP atau UDP
- Bendera koneksi TCP
- Jenis pesan ICMP lapisan jaringan

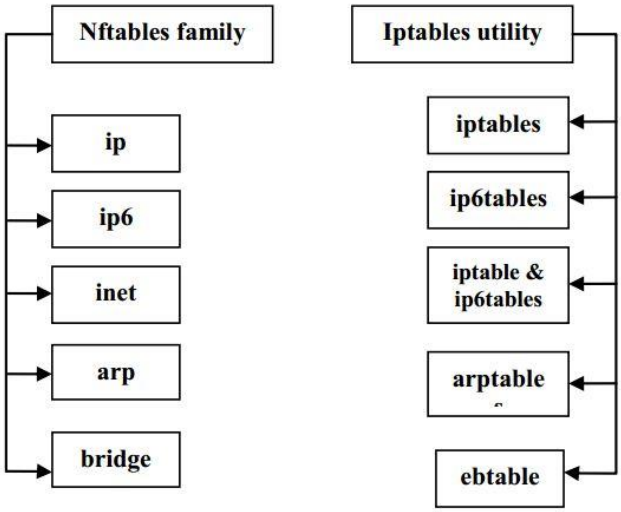
- Apakah paket masuk atau keluar

Jika paket cocok dengan kriteria aturan pertama, maka firewall melakukan tindakan yang dijelaskan oleh target. Jika paket tidak sesuai dengan kriteria, maka mesin pergi ke aturan berikutnya dalam rantai dan seterusnya. Jika firewall tidak memproses aturan dengan cukup cepat, seluruh sistem akan melambat. Filter paket tidak memeriksa bagian data paket. Urutan aturan didefinisikan penting sebagai proses firewall aturan dari atas ke bawah. Daftar aturan yang mendefinisikan apa yang bisa masuk dan apa yang bisa keluar disebut rantai.

2.2. Nftables

Nftables pertama kali diperkenalkan ke publik di *Netfilter Workshop 2008* oleh Patrick McHardy dari Tim Inti Netfilter. Peluncuran pratinjau pertama dari implementasi kernel dan *userspace* pada Maret 2009. Pada 16 Oktober 2013, Pablo Neira Ayuso mengajukan permintaan penarikan inti nftables ke pohon kernel utama Linux untuk digabung menjadi kernel utama pada 19 Januari 2014, dengan rilis kernel Linux versi 3.13 [11]. Meskipun alat ini telah disebut, "perubahan terbesar terhadap firewall Linux sejak diperkenalkannya iptables pada tahun 2001". Nftables diperkenalkan pada inti Linux 3.13. Nftables menggunakan infrastruktur netfilter, tetapi secara dinamis dimuat modul berbeda jika dibandingkan dengan iptables. NFtables sudah bisa menggantikan bagian-bagian fungsi tertentu dari netfilter. Nftables dikonfigurasi melalui utilitas ruang-pengguna nft sementara netfilter dikonfigurasi melalui utilitas iptables, ip6tables, arptables, dan kerangka kerja ebtables.

Keuntungan utama dari nftables atas iptables adalah seperti yang dijelaskan pada Gambar 6 yaitu penyederhanaan kernel Linux dan perintahnya, pengurangan duplikasi kode, pelaporan kesalahan yang ditingkatkan, dan eksekusi yang lebih efisien, penyimpanan dan perubahan bertahap dari aturan penyaringan. Iptables yang digunakan secara tradisional, ip6tables, arptables dan ebtables untuk IPv4, IPv6, ARP dan *Ethernet bridging*, masing-masing dimaksudkan untuk diganti dengan nft sebagai implementasi tunggal yang terpadu, NFTable menyediakan konfigurasi firewall di atas mesin virtual di-kernel.



Gambar 6. Perbandingan Struktur Iptables dengan NFTables

2.3. Wireshark

Wireshark merupakan salah satu dari sekian banyak *tools network analyzer* yang banyak digunakan oleh *network administrator* untuk menganalisa kinerja jaringannya termasuk protokol didalamnya. Wireshark banyak disukai karena *interface*-nya yang menggunakan *Graphical User Interface* (GUI) atau tampilan grafis. Wireshark mampu menangkap paket-paket data atau informasi yang melewati jaringan. Semua jenis paket informasi dalam berbagai format *protocol* pun akan dengan mudah ditangkap dan dianalisa. Karenanya tak jarang *tools* ini juga dapat dipakai untuk *sniffing* (memperoleh informasi penting seperti *password* email atau *account* lain) dengan menangkap paket-paket yang melewati jaringan dan menganalisanya.

2.4. Teknologi virtualisasi

Virtualisasi server adalah penggunaan perangkat lunak yang memungkinkan satu perangkat keras untuk menjalankan beberapa sistem operasi dan services pada saat yang sama, sedangkan *virtual server* adalah penggunaan perangkat lunak yang memungkinkan banyak perangkat keras untuk menjalankan satu sistem secara terpadu. Teknologi virtualisasi server ini bertujuan untuk menghindari pemborosan daya proses yang mahal atau dengan kata lain meningkatkan efisiensi serta mengoptimalkan penggunaan processor berinti lebih dari satu. Penghematan lain adalah biaya listrik karena hanya menggunakan satu atau sedikit server saja Banyak tipe *processor* yang mempunyai inti lebih dari satu, terutama pada server. Dengan melihat potensi prosessor yang mempunyai inti lebih dari satu tersebut, kita dapat memanfaatkannya untuk menjalankan aplikasi-aplikasi dan services secara bersamaan menggunakan teknik virtualisasi pada komputer server. Konsep *cluster high availability* yang terdapat pada virtualisasi server dapat mengurangi biaya dan menyederhanakan pengelolaan pelayanan teknologi informasi. *Processor* dengan inti lebih dari satu mempunyai kemampuan yang cukup untuk melakukan berbagai macam proses secara bersamaan, akan tetapi belum semua aplikasi pada saat ini yang dapat memanfaatkan secara optimal prosesor berinti banyak (*multi prosessor*) tersebut.

Berdasarkan pengamatan dari Tony Iams, analis senior di D.H. Brown Associates Inc, NY, server di sebagian besar organisasi hanya menggunakan 15-20% dari kapasitas sesungguhnya, tentu saja angka tersebut merupakan rasio yang jauh dari ideal. Dengan melihat potensi prosessor yang mempunyai inti lebih dari satu tersebut, dapat kita manfaatkan untuk menjalankan aplikasi aplikasi dan *services* secara bersamaan menggunakan teknik virtualisasi pada komputer *server*. Pada saat ini banyak sekali virtualisasi *server* menggunakan proxmox, vmware esx dan *openstack* yang merupakan tipe virtualisasi *server* yang *free* dan mudah dalam instalasi. Dalam penelitian ini penulis menggunakan VMware Esxi untuk media penelitiannya.

2.5. Denial of service (DoS)

Serangan DoS (*Denial-of service attacks*) adalah jenis serangan terhadap sebuah komputer atau server didalam jaringan internet dengan cara menghabiskan sumber (*resource*) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang

diserang tersebut. Penelitian yang dilakukan terkait *network forensics for detecting flooding attack on web server* [12], menjelaskan bahwa ancaman serius keamanan jaringan pada server web yang mengakibatkan hilangnya *bandwidth* dan kelebihan beban bagi pengguna dan *server web* penyedia layanan.

Jenis – jenis serangan DoS, diantaranya :

Ping Of Death

Merupakan serangan klasik yang dulu sering digunakan. Serangan ini di dilancarkan dengan menggunakan *utility* ping pada sebuah sistem operasi. Ping biasanya digunakan untuk memeriksa keberadaan sebuah host. Atau alamat IP dari sebuah website. Data yang dikirimkan secara default adalah 32 bytes, namun pada kenyataannya program ini dapat mengirimkan sampai dengan 65kb data. Sekarang serangan seperti ini sudah tidak terlalu ampuh lagi, karena banyak sistem yang telah meng *update patch*nya dan menutup lubang-lubang tersebut. Ditambah semakin canggihnya teknologi dan semakin lebarnya *bandwidth* yang tersedia, sehingga serangan ini tidak lagi menimbulkan dampak yang signifikan bagi sebuah sistem.

Syn flooding

Serangan *Syn Flooding* dilakukan dengan cara memanfaatkan kelemahan protokol pada saat terjadinya proses *handshake*. Saat dua buah komputer memutuskan untuk memulai melakukan komunikasi maka komputer pengirim (penyerang) akan mengirimkan *syn*, penerima (target) pun akan menjawab dengan mengirimkan *syn ack* kepada komputer pengirim. Seharusnya setelah menerima balasan *syn ack* dari pengirim ack kepada penerima untuk melakukan proses *handshake*. Namun pada kenyataannya, pengirim justru mengirikan banyak paket *syn* kepada penerima yang mengakibatkan penerima harus terus menjawab permintaan dari pengirim. Alamat IP penyerang biasanya telah disembunyikan atau *spoofed* sehingga alamat yang dicatat oleh target adalah alamat yang salah. Penerima akan bingung untuk menjawab permintaan koneksi TCP yang baru karena masih menunggu banyaknya balasan ack dari pengirim yang tidak diketahui tersebut. Disamping itu koneksi juga akan dibanjiri oleh permintaan *syn* yang dikirim oleh pengirim secara terus menerus. Serangan seperti ini menghambat penerima memberikan pelayanan kepada user yang absah.

Remote controled attack

Remote controled attack pada dasarnya adalah mengendalikan beberapa *network* lain untuk menyerang target. Penyerangan dengan tipe ini biasanya akan berdampak besar, karena biasanya server- server untuk menyerang mempunyai *bandwith* yang besar. Penyerang juga dengan leluasa dapat mengontrol dan menyembunyikan identitas diri dibalik server-server tersebut. Banyak *tools* yang dapat digunakan untuk melakukan serangan dengan tipe ini. Umumnya *tools-tools* tersebut mempunyai tipe master dan *client* atau *agent*. Master merupakan komputer master yang telah dikuasai oleh penyerang dan akan digunakan untuk memberikan perintah kepada para agent guna melancarkan serangan. Sedangkan *client* adalah komputer *zombie* yang telah berhasil dikuasai oleh penyerang, kemudian penyerang menanamkan aplikasi *client* yang siap menungu perintah untuk menyerang target. Tools yang cukup terkenal dari tipe serangan ini adalah trinoo.

UDP *flood*

Serangan UDP ini memanfaatkan protokol UDP yang bersifat *connectionless* untuk menyerang target. Karena sifatnya itulah UDP *flood* cukup mudah untuk dilakukan. Sejumlah paket data yang besar dikirimkan begitu saja kepada korban. Korban yang kaget dan tidak siap menerima serangan ini tentu akan bingung, dan pada beberapa kasus komputer server tersebut akan *hang* karena besarnya paket data yang dikirimkan. Penyerang dapat menggunakan tehnik *spoofed* untuk menyembunyikan identitasnya.

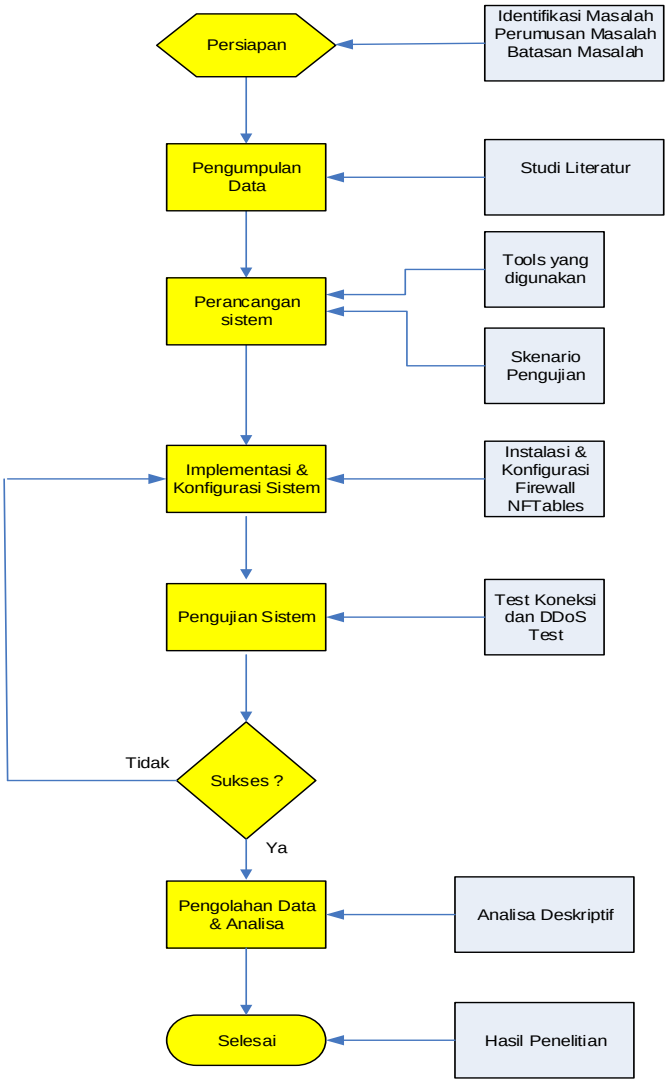
Smurf Attack

Merupakan penyerangan dengan memanfaatkan ICMP *echo request* yang sering digunakan pada saat mem*broadcast* identitas kepada *broadcast address* dalam sebuah *network*. Saat melakukan *broadcast* pada *broadcast address* maka semua komputer yang terkoneksi kedalam jaringan akan ikut menjawab *request* tersebut. Hal ini tentu saja akan melambatkan dan memadatkan trafik di jaringan karena komputer-komputer yang tidak ditanya turut memberikan *request* tersebut. Hal ini tentu akan berdampak lebih besar bila alamat pengirim *request* disamarkan, dan tidak hanya mengirimkan ICMP *request* pada sebuah *network* melainkan kebeberapa *network*. Tentu saja balasan yang diterima akan lebih besar lagi, tidak hanya sampai disitu saja. Pengirim akan menyamarkan identitasnya dengan cara memakai alamat IP orang lain, maka ia akan diserang dengan balasan icmp *echo request* dari beberapa *network* sekaligus.

3. METODE PENELITIAN

Obyek penelitian dari penulisan ini adalah kinerja sistem *firewall* yang di implementasikan pada mesin virtualisasi Vsphere Esxi untuk melayani dan mengamankan server-server yang ada di belakang firewall tersebut. Secara khusus obyek yang di implementasikandan diujikan performanya pada penelitian ini adalah *firewall* generasi baru yaitu *nftables* pada server mesin virtualisasi. *firewall* yang sudah dikonfigurasi selanjutnya akan dilakukan pengujian serangan DDoS untuk di analisa nilai *troughput* dari firewall tersebut.

Dalam penelitian ini dilakukan dalam beberapa tahap seperti tergambar dalam flowchart Gambar 7.



Gambar 7. Bagan alur Proses Penelitian

Tahapan alur proses penelitian adalah sebagai berikut:

a. Persiapan untuk eksekusi perumusan masalah
   Pada tahap ini berisi mengenai gambaran umum penelitian tentang identifikasi masalah, perumusan masalah, batasan masalah dan tujuan penelitian pada penerapan firewall nftables di lingkungan mesin virtualisasi.
b. Pengumpulan data
   Pada tahap ini dilakukan *study literature* terkait perangkat lunak yang digunakan dan teori-teori yang berkaitan dengan topik masalah yang diambil dan hal hal yang berguna dalam proses analisis permasalahan.
c. Perancangan sistem
   Tahapan ini memberikan informasi tentang kebutuhan perangkat, desain pengujian performa, informasi metodologi penelitian yang dilakukan, alat dan skenario yang digunakan dalam mengevaluasi firewall.
d. Implementasi dan Konfigurasi sistem
   Pada tahap ini dilakukan proses installasi firewall dan konfigurasi dimulai dari installasi dan konfigurasi sistem operasi linux, aplikasi firewall yaitu Nftables

serta aplikasi pengujian performa terhadap serangan DDoS (*Distributiion Denial of Service*) yang menggunakan seperti hping3.

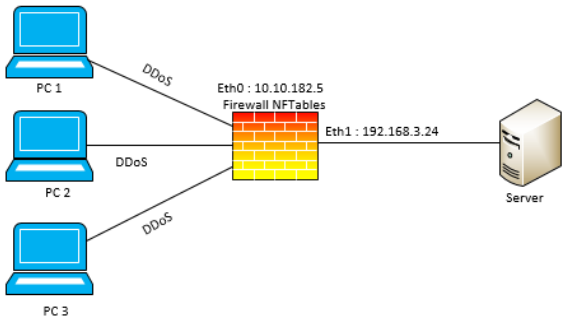
e. Pengujian system

Pada tahap ini dilakukan pengujian performa firewall dengan eksperimen penyerangan DDoS menggunakan 3 PC staff padakedua server firewall seperti pada Gambar 8 dan pengujian kedua menggunakan 6 PC seperti pada Gambar 9, pengujian ini untuk mengambil data nilai troughput. Skenario penyerangan dilakukan sebagai berikut:

SKENARIO 1

- Menggunakan 3 PC dari luar (depan) firewall untuk memberikan serangan DDoS (*Distribution Denial of Service*), masing-masing 3 PC paralel membombardir firewall nftables yang mempunyai IP Address "10.10.182.5" dengan ICMP *echo request*.
- Jumlah serangan komputer penyerang adalah 50 kali (50 detik) tiap PC nya, serta jumlah ping paket tiap PC adalah 3200 byte, jadi total serangan ke server Firewall sebanyak 96000 byte.
- Jarak antar paket di setting 10 ms
- Perintah yang digunakan melalui command prompt dari komputer penyerang adalah:

hping3 -c 1000000 -d 3200 -S -w 64 --flood --rand-source 10.10.182.5
Catatan: 10.10.182.5 adalah IP Adrees firewall nftables

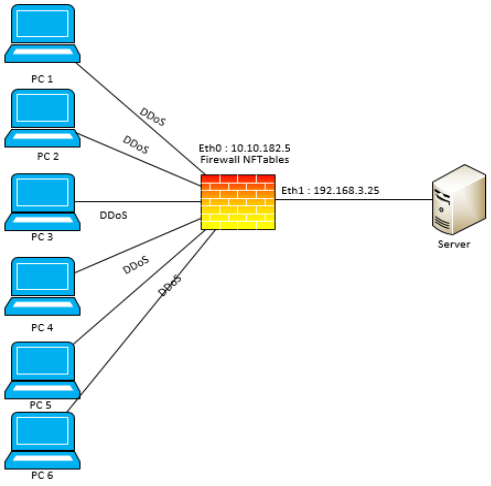


Gambar 8. Desain Topologi pengujian firewall dengan serangan DDoS dari 3 PC.

SKENARIO 2

- Menggunakan 6 PC dari luar (depan) *firewall* untuk memberikan serangan DDoS (*Distribution Denial of Service*), masing-masing 6 PC membombardir firewall nftables yang mempunyai IP Address "10.10.182.5" dengan ICMP *echo request*.
- Jumlah serangan komputer penyerang adalah 50 kali (50 detik) tiap PC nya, serta jumlah paket ping setiap komputer penyerang adalah 65000 bytes, jadi total serangan ke server firewall sebanyak 325000 bytes.
- Jarak antar paket di setting 900 ms.
- Perintah yang digunakan melalui command prompt dari komputer penyerang adalah:

hping3 -c 1000000 -d 65000 -S –w 64 --flood --rand-source 10.10.182.5 (catatan : server 10.10.182.5 adalah alamat server firewall NFTables)



Gambar 9. Desain Topologi pengujian firewall dengan serangan DDoS dari 6 PC.

Setelah data dicatat dan dikumpulkan kemudian di buat tabel dan grafiknya serta ditentukan rata-rata *troughput*nya dari setiap skenario. Kemudian data tersebut di bandingkan untuk dianalisa.

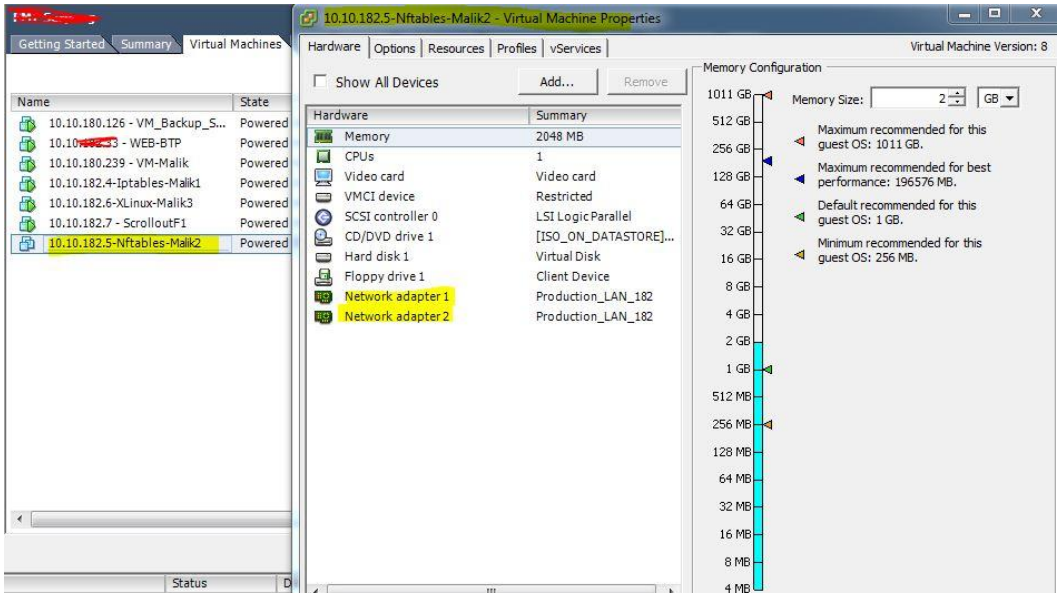
4. IMPLEMENTASI DAN ANALISA

4.1. Implementasi

Tahapan implementasi sistem merupakan tahap penerjemahan penerapan sistem berdasarkan hasil analisis serta penerapan kebutuhan pada keadaan yang sebenarnya.

Dalam penelitian ini penulis menggunakan komputer server fisik yang sudah terinstall system operasi Vsphere ESXi, dimana didalam sistem operasi Vsphere tersebut terdapat beberapa komputer virtualiasi yang dibuat dalam bentuk *host*, *cluster* atau *single VM* seperti pada Gambar 10, adapun spesifikasi server fisik mesin virtualisai adalah sebagai berikut:

- Processor Intel Xeon 4C E3-1220V2 3.1G 8M 5GT/s DMI
- Harddisk 3x 2TB SATA 3.0 with RAID 5
- RAM 16 GB
- 2x Ethernet GigaByte



Gambar 10. Implementasi perangkat keras firewall NFTables dalam mesin virtualisasi.

Spesifikasi perangkat lunak yang digunakan terbagi menjadi 3 bagian yaitu :

a. Perangkat lunak untuk sistem operasi yang digunakan pada *firewall* nftables disini adalah Linux Ubuntu 18.04 kernel 4.15.

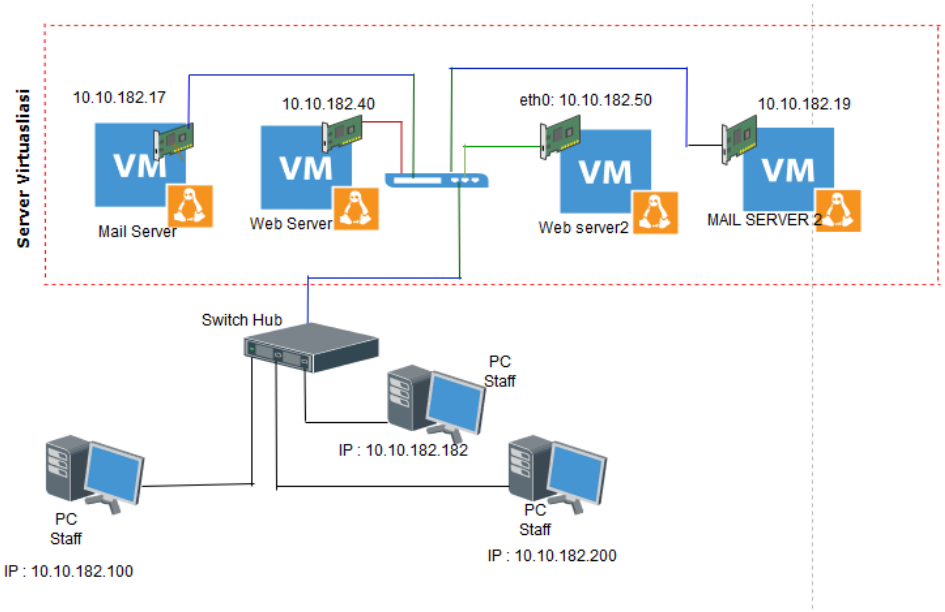
b. Perangkat lunak untuk aplikasi firewall yang digunakan yaitu nftables versi 0.8.2 dengan konfigurasi anti DDoS seperti pada Gambar 11.

```
if [[ $SCALE -eq 0 ]]; then
        nft add table netdev t
        nft add chain netdev t c \
             '{ type filter hook ingress device enp3s0 priority 0; }'
        nft add chain netdev t test
        nft add rule netdev t c jump test
        nft add rule netdev t c accept
else
        for j in {1..10}; do
                nft add rule netdev t test ip saddr 10.10.182.$SCALE.$j drop
        done
fi
```

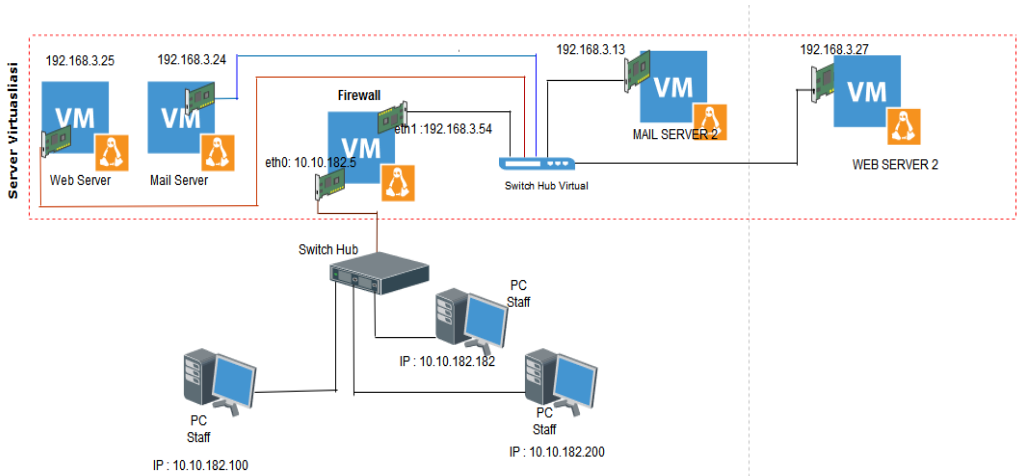
Gambar 11. Konfigurasi anti DDoS yang diterapkan di firewall NFTables

c. Perangkat lunak untuk pengujian atau evaluasi performa kinerja *firewall*, yaitu hping3. Selain alat pengujian yang disebutkan, firewall juga akan dimonitor oleh *capture* jaringan seperti *wireshark* dan tcpdump.

Salah satu persiapan dalam membangun sistem keamanan server di mesin virtualisasi adalah menyiapkan konsep arsitektur jaringan. Perancangan jaringan dengan topologi baru pada server mesin virtualisasi, dimana yang sebelumnya server-server di mesin virtuliasasi terhubung langsung dengan jaringan LAN staff seperti dijelaskan pada Gambar 12 setelah pada penelitian ini dibuatkan VM *Firewall* Nftables pada server mesin virtualisasi tersebut, maka lalu lintas data server akan seperti Gambar 13, yaitu semua traffic akan melewati VM *firewall* nftables terlebih dahulu.



Gambar 12. Topologi jaringan server pada mesin virtualisasi di Balai Teknologi Polimer sebelum menggunakan Firewall



Gambar 13. Topologi jaringan server di mesin virtualisasi Balai Teknologi Polimer setelah menggunakan firewall

4.2. Analisa Uji serangan DDoS

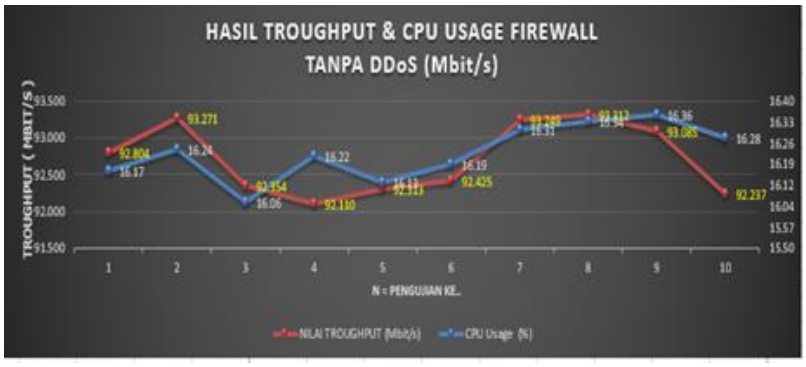
Pada penelitian ini pengambilan data di ambil sebanyak 30 kali dimana data awal sebanyak 10 kali pengambilan data *paket per second* (pps) troughput tanpa adanya serangan DDoS sebagai data acuan kualitas awal dari layanan sistem firewall. Selanjutnya diambil data troughput sebanyak 10 kali dengan skenario 1, penyerangan dengan menggunakan 3 komputer dengan masing-masing menyerang dengan data *size* 32000 bytes. Terakhir adalah skenario 2 dengan menggunakan 6 komputer dan masing-masing komputer menyerang dengan data *size* sebanyak 65000 bytes, dari pengujian pada scenario 1 dan 2 juga dipantau penggunaan *resource* atau sumber daya yang terpakai pada CPU *prosessor* saat tidak ada dan sudah ada serangan DDoS (*Distribution Denial of Service*).

Pengambilan nilai troughput tanpa adanya serangan DDoS dilakukan sebanyak 10 kali dengan menggunakan htping3 dan *software capture* jaringan yaitu Wireshark**,** didapat hasil seperti Tabel 1.

Tabel 1. Nilai *Troughput* Percobaan Tanpa serangan DdoS

No.	Pengujian	Cpu Usage (%)	Nilai Troughput (Mbit/S)
1	N1	16.17	92.804
2	N2	16.24	93.271
3	N3	16.06	92.354
4	N4	16.22	92.110
5	N5	16.13	92.313
6	N6	16.19	92.425
7	N7	16.31	93.249
8	N8	16.34	93.312
9	N9	16.36	93.085
10	N10	16.28	92.237

Dari hasil percobaan tanpa serangan DDoS seperti yang tertera di Tabel 1 didapat nilai rata-rata *Troughput* sebesar 92,716 Mbit/sec, dan rata-rata *CPU Usage* (%) nya adalah 16,23 %. Grafik nilai Troughput dan CPU Usage tanpa serangan DDoS adalah seperti grafik Gambar 14.



Gambar 14. Grafik Nilai Troughput dan CPU Usage Tanpa Serangan DDoS

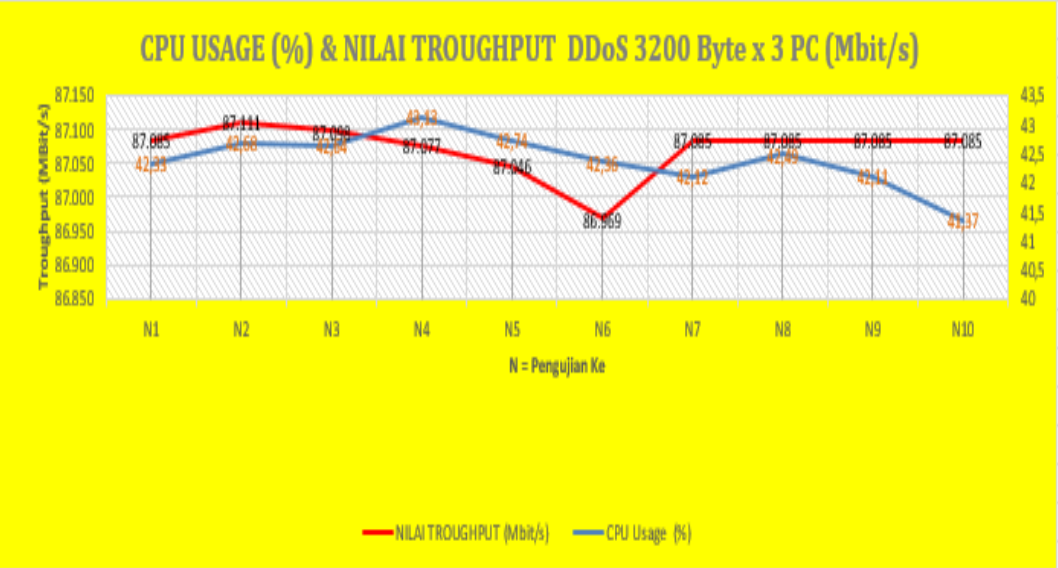
Skenario 1 adalah dimana akan dilakukan serangan ke server firewall NFTables dengan menggunakan 3 komputer yang masing-masing melakukan ping sebanyak 32000 bytes yang kemudian diambil data nilai troughput dan penggunaan sumber daya *prosessor*nya. Dari hasil pengujian di dapat nilai troughput dan *CPU Usage* (%) seperti Tabel 2.

Tabel 2. Nilai Troughput Dengan DoS 32000 bytes sebanyak 3 PC

No	Pengujian	Cpu Usage (%)	Nilai Troughput (Mbit/S)
1	N1	42,33	87.085
2	N2	42,68	87.111
3	N3	42,64	87.098
4	N4	43,13	87.077
5	N5	42,74	87.046
6	N6	42,36	86.969
7	N7	42,12	87.085
8	N8	42,49	87.085
9	N9	42,11	87.085
10	N10	41,37	87.085

Dari hasil percobaan dengan serangan DDoS dengan Htping3 melalui 3 komputer penyerang sebanyak 32000 bytes seperti yang tertera pada Tabel 2 didapat nilai rata-rata *troughput* sebesar 87,073 Mbit/sec dan rata-rata CPU *Usage* server firewall sebesar 42, 397 %.

Grafik nilai *troughput* dan CPU *Usage* dengan serangan DDoS dengan Htping3 melalui 3 komputer penyerang sebanyak 32000 bytes adalah seperti grafik Gambar 15.



Gambar 15. Grafik nilai troughput dan CPU Usage (%) dari DDoS 3 Komputer.

Skenario 2 adalah dimana akan dilakukan serangan ke firewall nftables dengan menggunakan 6 komputer yang masing-masing melakukan Htping3 sebanyak 65000 bytes yang kemudian diambil data nilai penggunaan sumber daya prosessor dan nilai *troughput*nya.

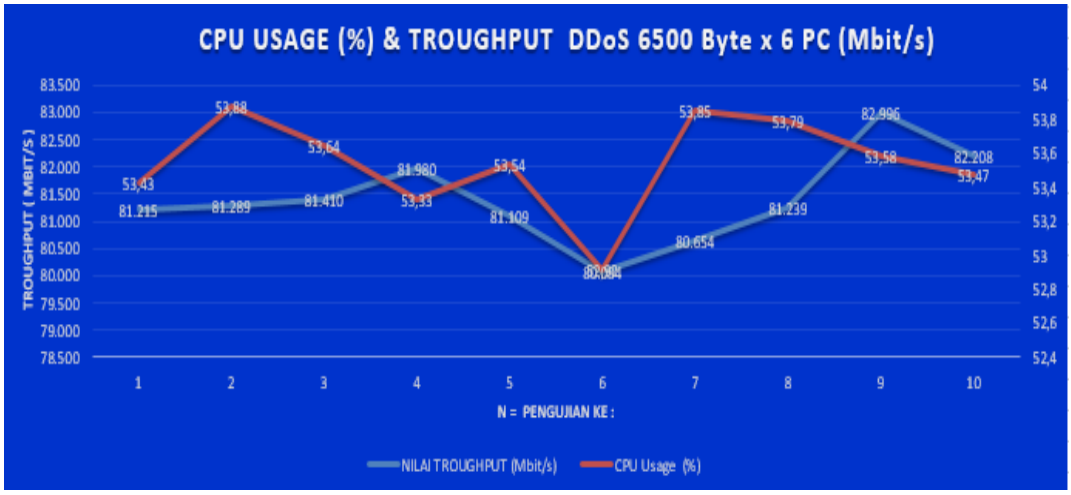
Dari hasil pengujian dengan serangan DDoS dengan Htping3 melalui 6 komputer penyerang sebanyak 65000 bytes didapat nilai rata-rata Troughput sebesar 81, 418 Mbit/sec dan CPU *usage* firewall sebesar 53, 543 %.

Detail dari hasil pengujian di dapat nilai troughput dan CPU usage seperti pada Tabel 3.

Tabel 3. Nilai Troughput & CPU Usage (%) dari DDoS 6 PC

No	Pengujian	Cpu Usage (%)	Nilai Troughput (Mbit/S)
1	N1	53,43	81.215
2	N2	53,88	81.289
3	N3	53,64	81.410
4	N4	53,33	81.980
5	N5	53,54	81.109
6	N6	52,92	80.084
7	N7	53,85	80.654
8	N8	53,79	81.239
9	N9	53,58	82.996
10	N10	53,47	82.208

Adapun grafik nilai *Troughput* dan CPU Usage dengan serangan DDoS menggunakan htping3 melalui 6 komputer penyerang sebanyak 65000 bytes adalah seperti grafik Gambar 16.



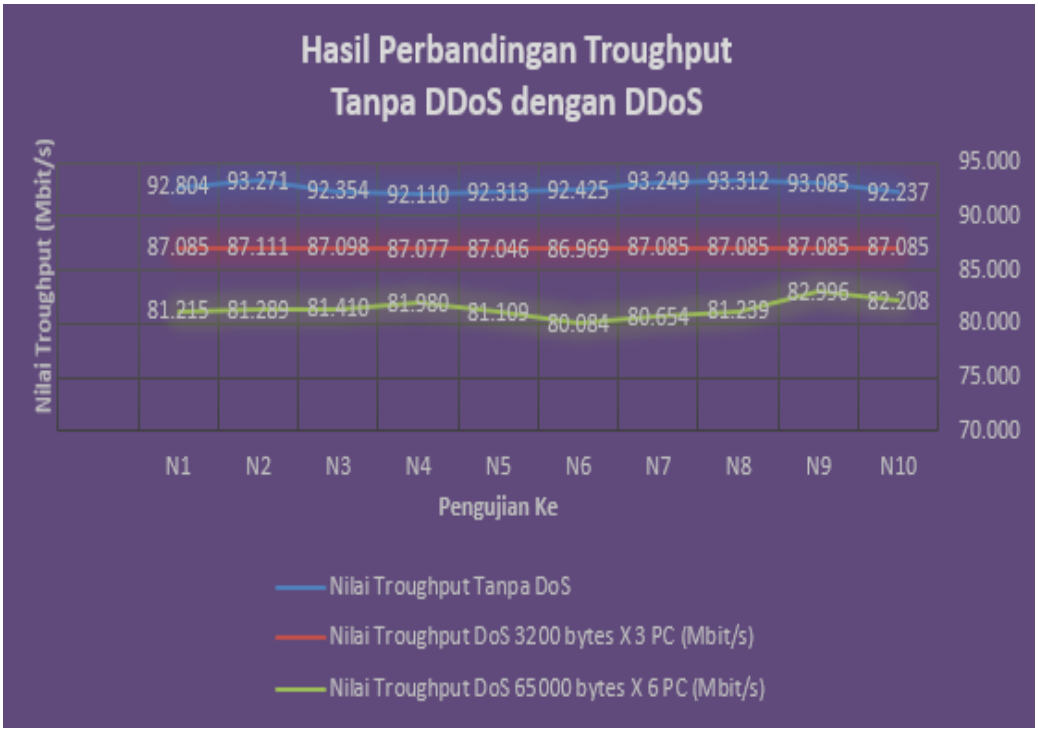
Gambar 16. Grafik Nilai *Troughput* dan CPU Usage (%) DDoS 6 Komputer

Dari hasil pengujian-pengujian yang kemudian di rangkum menjadi sebuah tabel dan grafik agar dapat di analisa fenomena yang ada. Hasil pengujian troughput diatas didapatkan tabel seperti Tabel 4.

Tabel 4. Tabel perbandingan Nilai Troughput

Pengujian Ke	Nilai Troughput Tanpa Ddos	Nilai Troughput Ddos 3 Pc (Mbit/S)	Nilai Troughput Ddos 6 Pc (Mbit/S)
N1	92.804	87.085	81.215
N2	93.271	87.111	81.289
N3	92.354	87.098	81.410
N4	92.110	87.077	81.980
N5	92.313	87.046	81.109
N6	92.425	86.969	80.084
N7	93.249	87.085	80.654
N8	93.312	87.085	81.239
N9	93.085	87.085	82.996
N10	92.237	87.085	82.208
Rata-Rata	**92.716**	**87.073**	**81.418**

Kemudian dari Tabel 4 didapat grafik seperti Gambar 17.



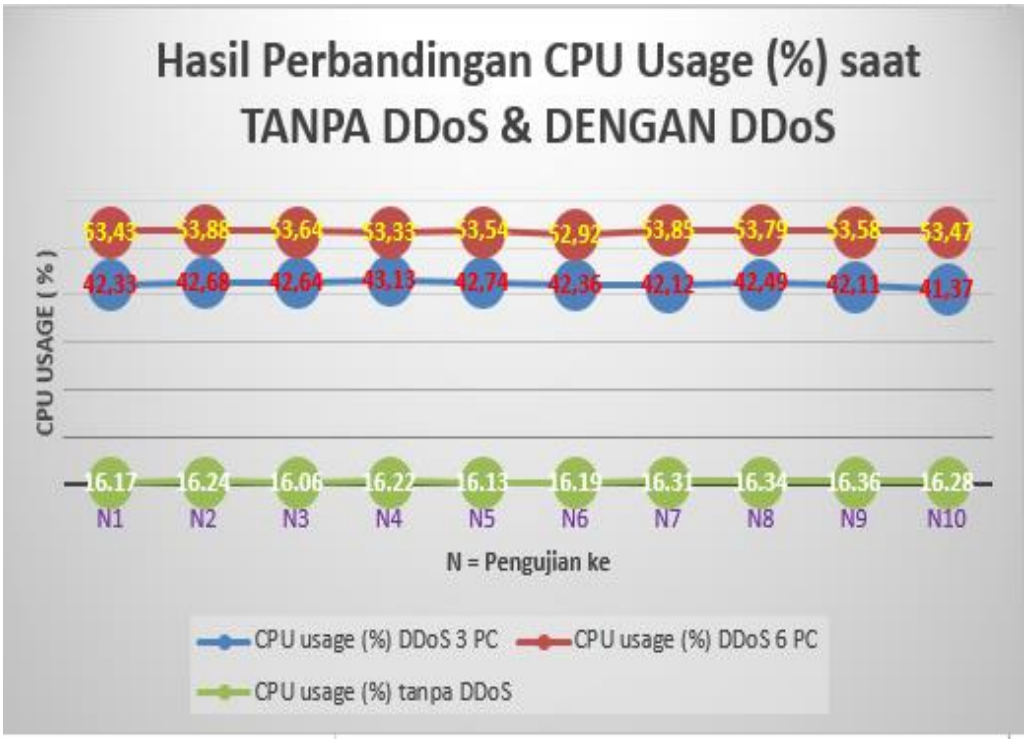
Gambar 17. Grafik nilai troughtput dari hasil 3 pengujian serangan DDoS

Dan dari hasil pengujian-pengujian pengaruh serangan DDoS terhadap penggunaaan sumber daya prosessor *(CPU Usage)* server firewall Nftables dijelaskan juga dalam tabel dan grafik agar dapat di analisa fenomena yang ada, seperti dipaparkan pada Tabel 5 berikut ini ini.

Tabel 5. Tabel perbandingan CPU Usage (%)

Pengujian Ke	Cpu Usage Tanpa Ddos (%)	Cpu Usage Ddos 3 Pc (%)	Cpu Usage Ddos 6 Pc (%)
N1	16.17	42,33	53,43
N2	16.24	42,68	53,88
N3	16.06	42,64	53,64
N4	16.22	43,13	53,33
N5	16.13	42,74	53,54
N6	16.19	42,36	52,92
N7	16.31	42,12	53,85
N8	16.34	42,49	53,79
N9	16.36	42,11	53,58
N10	16.28	41,37	53,47

Kemudian dari Tabel 5 didapat garfik seperti Gambar 18.



Gambar 18. Grafik nilai CPU Usage (%) dari pengujian serangan DDoS

Dari data hasil pengujian DDoS pada firewall diatas dapat terlihat:

- Rata-rata *Troughput* tanpa serangan DDoS adalah sebesar 92.716 MBit/sec, dan rata-rata CPU *Usage* pada server firewall NFTables saat tanpa DDoS adalah 16,23 %.
- Rata-rata Troughput dengan serangan DDoS 32000-byte x 3 PC adalah sebesar 87,073 MBit/sec terjadi penurunan sebesar 6,08% dari keadaan normal. Dan rata-rata CPU *Usage* nya dari DDoS 3 PC tersebut adalah 42,397%, terjadi Kenaikan penggunaan sumber daya prosessor firewall sebesar 61,71%
- Rata-rata troughput dengan serangan DDoS 65000 byte x 6 PC adalah sebesar 81.418 MBit/sec, terjadi penurunan sebesar 12,185 % dari keadaan normal. Dan rata-rata CPU *Usage* nya dari DDoS 6 PC tersebut adalah 53,543%, terjadi kenaikan penggunaan sumber daya prosessor firewall sebesar 69,69 **%**
- Jadi dengan serangan DDoS yang dilakukan terjadi penurunan tingkat Troughput dan kenaikan penggunaan sumber daya prosessor, walaupun masih bisa berjalan baik dengan pengamatan langsung tetapi hal ini harus menjadi perhatian sehingga tidak menjadi kendala nantinya.

Terjadi penurunan nilai troughput atau kualitas layanan setelah mendapat serangan DDoS adalah sesuai dengan para peneliti yang mengatakan "Serangan DDoS membuat sistem atau layanan jaringan tidak tersedia untuk pengguna yang sah. Serangan ini merupakan gangguan minimal, atau dapat serius merusak jika sistem kritis adalah korban utama. Kehilangan sumber daya jaringan menyebabkan kerugian ekonomi, keterlambatan pekerjaan, dan hilangnya komunikasi antara pengguna jaringan [13].

5. KESIMPULAN

Setelah dilakukan implementasi dan analisa kualitas jaringan server firewall nftables didalam mesin virtualiasi yang ada di Balai Teknologi Polimer, maka dapat diambil beberapa kesimpulan sebagai berikut:

a. Sistem firewall didalam mesin virtualisasi yang sudah di implementasikan dapat menambah keamanan layanan server yang ada dibelakangnya, dan server yang ada dibelakang firewall tetap dapat dengan mudah diakses setiap saat.
b. Melalui pengukuran *troughput* dan penggunaan sumber daya pada firewall nftables, terjadi sedikit penurunan performa pada firewall karena adanya gangguan DDoS *(Distribution Denial of Service)* yang dilakukan beberapa komputer, semakin besar jumlah gangguan dan jumlah penyerang semakin menurunkan nilai *troughput* dari layanan server yang berada dibelakang *firewall* yang dibangun.
c. Rata-rata Troughput dengan serangan DDoS 32000-byte x 3 PC adalah sebesar 87,073 MBit/sec terjadi penurunan sebesar 6,08 % dari keadaan normal. Dan rata-rata CPU *Usage* nya dari DDoS 3 PC tersebut adalah 42,397 %, terjadi Kenaikan penggunaan sumber daya prosessor firewall sebesar 61,71 %
d. Rata-rata troughput dengan serangan DDoS 65000-byte x 6 PC adalah sebesar 81.418 MBit/sec, terjadi penurunan sebesar 12,185 % dari keadaan normal. Dan rata-rata CPU *Usage* nya dari DDoS 6 PC tersebut adalah 53,543%, terjadi kenaikan penggunaan sumber daya prosessor firewall sebesar 69,69 %
e. Dalam perbandingan penggunaan *firewall* atau tidak menggunakan *firewall*, masih lebih baik menggunakan firewall dalam hal performa server terhadap serangan DDoS, dalam hal ini *rule firewall* anti DDoS yang dikonfigurasi juga sudah berfungsi dengan baik, meminimalisir jumlah serangan ICMP *request* yang membanjiri firewall, dimana firewall masih dapat bekerja dengan baik walaupun sumber daya prosessor mengalami kenaikan.
f. Server firewall yang di implementasikan kemungkinan masih mempunyai celah keamanan dan kelemahan karena secara fisik server firewall berada di mesin virtualisasi, bukan berupa *single* server atau server fisik tersendiri.
g. Terkadang implementasi firewall dengan server fisik, akan lebih bagus performanya daripada di mesin virtualisasi, namun perlu digaris bawahi bahwa pada dasarnya, kinerja jaringan dari firewall tidak hanya ditentukan oleh seberapa tinggi spesifikasi perangkat kerasnya, tetapi juga bergantung pada konfigurasi atau algoritma yang optimal.

REFERENCES

[1] L. Lemus-Zúñiga, J. Benlloch-Dualde, J. M. Montañana, M. A. M. Pla and J. Pons, Teaching computer networks using virtual machines, *2015 International Conference on Information Technology Based Higher Education and Training (ITHET)*, Lisbon, 2015, pp. 1-6. doi: 10.1109/ITHET.2015.7218026

[2] J. Sitompul. (2012). *Cyberspace, Cybercrimes, Cyberlaw Tinjauan Aspek Hukum Pidana*. Jakarta: Tatanusa.

[3] A. Fadlil, I. Riadi, and S. Aji, Development of Computer Network Security Systems So That Network Forensic Analysis, *J. Ilmu Tek. Elektro Komput dan Inform*., Vol. 3, No. 1, pp. 11–18, 2017.

[4] T. Jonsson, *Latency and throughput comparison between iptables and nftables at different frame and rule-set sizes,* 2018.
[5] M. Nazir, *Metodologi Penelitian*. Ghalia Indonesia. Jakarta. 2003
[6] I. P. A. Pratama, *Smart City Beserta Cloud Computing dan Teknologi-teknologi pendukung lain-nya*. Bandung. Informatika. 2014.
[7] W. Stallings, *Network and Internetwork Security*, Prentice Hall, 2012
[8] M. Curtin, J. Ranum, and J. Markus, *Internet Firewalls: FAQ*. Rev 10, 2000.
[9] I. Cartealy, *Linux Networking*. Indonesia: Jasakom. 2013.
[10] G. Sondakh, E. I. Meicsy, I. Najoan, A. S. Lumenta, *Perancangan Filtering Firewall Menggunakan Iptables Di Jaringan Pusat Teknologi Informasi Unsrat*, 2014.
[11] L. García. *Load Balancing with nftables*, 2016.
[12] D. Mualfah and I. Riadi, Network Forensics for Detecting Flooding Attack on Web Server, IJCSIS, Vol. 15, No. 2, pp. 326–331, 2017.
[13] K. Chauhan, V. Prasad, Distributed Denial of Service (DDoS) Attack Techniques and Prevention on Cloud Environment, *International Journal of Innovations & Advancement in Computer Science, pp. 210-215, 2015.*